REDLEGG

Industry:
Manufacturing

Client Since:
2023

CASE STUDY

Scaling Security Automation in Enterprise Environments

INTRODUCTION

Security automation can create meaningful efficiency for teams managing high alert volume, expanding toolsets, and pressure to improve response without adding headcount. But the value of automation depends on how well it supports daily security work: the workflows analysts follow, the systems they rely on, and the decisions they need to make during an investigation.

Automation has become essential to maintaining operational efficiency at scale.
Albemarle had already invested in **XSOAR** to support its automation efforts. But like many organizations, deploying the platform was only the first step. Unlocking meaningful value from it required more than access; it required strategy, expertise, and operational alignment.

Effective automation depends on reducing manual effort, improving consistency, and helping analysts focus on higher-value work.

Despite having the platform in place, workflows still required manual effort, processes remained disconnected, and scaling automation across real use cases proved more difficult than expected.

The objective was to help Albemarle expand automation in a way that supported real operational workflows.

THE PROBLEM

Several high-value processes still depended on manual steps. User monitoring, for example, required analysts to run multiple queries across different systems to gather activity for a single user. Other investigations required analysts to move between tools to collect vulnerability context, review endpoint data, or complete response actions.

That fragmentation limited the efficiency Albemarle wanted from XSOAR. Data existed across the environment, but it was not always centralized inside the workflows analysts used to investigate and respond. As a result, analysts still spent time gathering context, repeating queries, and moving between platforms before they could make decisions.

These challenges weren't isolated issues. They pointed to a broader gap between having automation in place and making it operational across the environment.

MANUAL LOAD

CRITICAL WORKFLOWS STILL REQUIRED ANALYST-DRIVEN EFFORT.

FRAGMENTED PROCESSES

SECURITY TASKS RELIED ON MULTIPLE DISCONNECTED SYSTEMS.

LIMITED SCALE

AUTOMATION EXISTED, BUT WASN'T DELIVERING CONSISTENT EFFICIENCY.

Scaling automation also introduced its own complexity. Effective SOAR workflows need to account for integrations, API limitations, changing platforms, exception handling, and analyst handoffs. Without dedicated automation expertise and ongoing refinement, individual playbooks can become difficult to maintain or fail to deliver the efficiency teams expect.

> **"The goal was to take the workflows they already had and make them work reliably in day-to-day operations."**
> — Andrew Hale, SecOps Engineering & Automation Manager

WHY REDLEGG

RedLegg had previously supported Albemarle through Managed SIEM services, giving the engagement an established understanding of the environment and operational workflows. As Albemarle's needs evolved toward automation optimization, RedLegg was positioned to provide the expertise needed to support those efforts inside the existing XSOAR environment.

Through a flexible retainer model, RedLegg worked alongside Albemarle's internal team to build, refine, and optimize workflows aligned to real analyst operations and investigation processes.

As one Albemarle team member explained:

"Miguel and Andrew were always willing to listen to our ideas and help make our workflows more efficient."

SOLUTION / AUTOMATION WORKFLOW

RedLegg helped Albemarle centralize security workflows inside XSOAR by optimizing automation around recurring analyst tasks.

The work focused on user monitoring, alert enrichment, duplicate incident handling, email blocking workflows, and ticketing processes across existing systems.

Analysts previously had to move between multiple tools to gather context and complete response actions. RedLegg helped centralize those workflows inside XSOAR to support more efficient investigations.

RedLegg also improved response actions inside XSOAR, helping reduce tool switching and centralize investigation data across workflows.

INGESTION

Relevant activity is gathered from connected systems into XSOAR

ENRICHMENT

Additional context. including vulnerability and endpoint data, is pulled into the workflow.

ANALYST REVIEW

Analysts review centralized information instead of repeating queries across tools.

RESPONSE ACTIONS

Playbook actions support blocking, ticket updates, duplicate handling, and remediation workflows.

ONGOING REFINEMENT

Workflows are adjusted as systems. APIs, and operational needs change.

IMPLEMENTATION

RedLegg worked directly within Albemarle's XSOAR environment to build and refine automation workflows around real operational needs.

Many workflows required iterative testing and refinement based on evolving analyst requirements, integration challenges, and changing systems.

This included improving duplicate incident handling, refining email-related workflows, and adapting workflows around API limitations and platform changes.

> **"RedLegg is helping us build an automation in XSOAR to avoid those extra queries and gather the information in one place."**
> — Tony D'Agostino, Albemarle

THE BENEFITS

By scaling automation across key workflows, Albemarle reduced manual effort and improved operational efficiency across security operations.

RedLegg helped centralize investigation data inside XSOAR, reducing tool switching and repetitive analyst tasks during investigations and response actions.

Workflow optimizations also improved consistency, streamlined case handling, and enabled analysts to focus on higher-value work.

> **"It's probably saving us an extra five minutes per incident. It's one less place I have to go, and it definitely reduces the tediousness."**
> — Tony D'Agostino, Albemarle

HOW IT WAS DELIVERED

CROSS-PLATFORM WORKFLOWS

Integrated XSOAR with existing security, ticketing, and response tools to reduce manual handoffs.

ITERATIVE REFINEMENT

Workflows continuously adapted based on testing, operational feedback, and evolving analyst requirements.

CUSTOM AUTOMATION LOGIC

Built workflows aligned to real analyst processes, exception handling, and incident response needs.

CONCLUSION

Albemarle's automation journey reflects a common reality in modern security operations: having the right platform is only the starting point. The real challenge is turning automation into something operational, scalable, and aligned to the way analysts actually work.

Through a co-managed approach, RedLegg helped Albemarle build and refine workflows that reduced manual effort, improved consistency across investigations, and centralized more response actions inside XSOAR.

By focusing on practical workflows and continuous refinement, Albemarle was able to improve operational efficiency, reduce tool switching, and create a more effective automation program that better supported daily security operations.

> **"Automation delivers greater value over time as processes become more connected, consistent, and scalable."**

— Andrew Hale
SecOps Engineering & Automation Manager

IMPACT

- **Reduced manual effort:** Minimized repeated queries, manual lookups, and repetitive incident handling.
- **Less tool switching:** Brought more context and response actions into XSOAR.
- **Improved analyst efficiency:** Helped analysts complete investigations more efficiently through centralized workflows.
- **Centralized investigation data:** Helped analysts review user activity and related context in one workflow.
- **Operational continuity:** Adapted workflows as Albemarle's systems and requirements changed.
- **Higher-value analyst focus:** Gave the internal team more time for investigation, decision-making, and security priorities.

FOR MORE INFORMATION REACH OUT:

312.757.4941

dotell@redlegg.com

redlegg.com

REDLEGG